The New Ethical Trilemma: Security, Privacy and Transparency

Jean-Gabriel Ganascia

The New Ethical Trilemma: Security, Privacy and Transparency

Jean-Gabriel Ganascia
LIP6 - University Pierre et Marie Curie - Sorbonne Universités
B.C. 169, 4, place Jussieu, 75252, Paris, Cedex 05, FRANCE
Jean-Gabriel.Ganascia@lip6.fr

July 21, 2011

Abstract

Numerous ethical and societal issues are related to the development of nanotechnology. Among them, the risk for privacy has long been discussed. Some people say that technology is neutral and that it does not really change the nature of problems, which are mainly political, while others state that its contemporary developments considerably amplify them; there are even persons who assert that it will make privacy protection obsolete. This paper discusses those different positions by making reference to the classical Panopticon that is an architecture for surveillance, which characterizes the total absence of privacy. It envisages the possible evolutions of the Panopticon due to the development of nanotechnologies. It shows that the influence of nanotechnology on privacy concerns cannot be dissociated from the influence of computers and biotechnologies, i.e. from what is currently called the NBIC convergence. Lastly, it concludes on the new ethical trade-off that has to be made between three contradictory requirements that are security, transparency and privacy.

Keywords: **N**ano-Panopticon Nanotechnology Panopticon Privacy Security Sousveillance Surveillance Transparency

Résumé

Le développement des nano-technologies soulève de nombreuses questions d'ordre éthique et sociétal. Parmi elles, celles qui portent sur la protection de la vie privée ont fait l'objet de nombreux débats. Certains pensent que les technologies sont neutres et qu'elles ne changent pas fondamentalement les problèmes qui sont d'ordre politique, tandis que d'autres prétendent que les développements techniques contemporains les amplifient considérablement. Il existe même des personnes qui affirment que la protection de la vie privée devient obsolette. Cet article discute ces différentes positions en faisant référence à l'architecture classique du Panopticon qui a été conçue pour faciliter la surveillance et qui se caractérise comme un totale privation de vie privée. Il envisage les évolutions possibles du Panopticon dues au développement des nanotechnologies. Il montre que l'influence des nanotechnologies sur tout ce qui concerne la vie privée ne peut être dissociée de celle des ordinateurs et des biotechnologies, c'est-à-dire de ce que l'on a coutume de désigner comme la convergence NBIC. Enfin, cet article conclut sur le nouveau compromis qui doit

tre trouvé entre les trois exigences contradictoires que sont la sécurité, la transparence et la protection de la vie privée.

Mots-clefs: **n**ano-panopticon nanotechnologies Panopticon vie privée sécurity sousveillance surveillance transparence

1 Ethical, Legal and Social Aspects of Nanosciences

1.1 Nanoethics

By *Nanoethics* (Marano, Lahmani & Houdy 2011) one generally understands anything that touches the ethics relative to the proliferation of nanoscale objects. This term is now official in the scientific community and it refers to a well-defined field of applied ethics. It has been deliberately coined to resemble the words 'bioethics' and 'roboethics' that now seem to be used by scientists in publications, by universities, by professional associations, and so on. There even exists a journal entitled 'NanoEthics' published by Springer[1]. Note that the subtitle of this journal, *Ethics for Technologies that converge at the nanoscale*, clearly stipulates that nanoethics is directly connected with converging technologies, i.e. with the notion of NBIC — that is the acronym for *Nanotechnology, Biotechnology, Information technology and Cognitive science* — introduced into public discourse through the (Roco & Bainbridge 2003) report sponsored by the United-States National Science Foundation and entitled *Converging Technologies for Improving Human Performance*.

1.2 Main Issues: From Nano-toxicity to Privacy

"Nano-ethical" development of nanotechnology requires to address various issues that belong to three main categories: nano-toxicity, environment protection and privacy.

Nano-toxicity (Marano et al. 2011) covers the effects of ingestion or inhalation of nanoparticles on health. Some scientists fear that substances, which are benign by themselves become malignant when spread in the form of nanoparticles (Stern & McNeil 2008). They allege that, because of their extremely small size, nanoparticles can invade and infect the lungs and that they can also cross through nasal cavities into the brain or via the placenta into developing fetuses. For instance, while gold dust is relatively safe, gold nanoparticles seem to be biologically active and to trigger intense chemical reactions.

Ecotoxicity, i.e. the potential danger of nanotechnologies for the environment has also been pointed out by numerous scientists. While it was proposed to use nanoscale iron to decontaminate the soil and the water (e.g. (Hillie & Hlophe 2007)) or to clean up clothes and surfaces contaminated with biological agents, some have argued that nanotechnologies could pose risks for our environment. For instance, titanium dioxide, which is usually a non-reactive substance that is present in many products like house paint, becomes chemically active under the form of nanoparticles. It can then burn bacteria. It could also accumulate in animal organs and lead to unanticipated consequences for those animals which might be passed to humans.

[1] cf. `http://www.springer.com/social+sciences/applied+ethics/journal/11569`

According to some visionaries authors (e.g. (Joy 2000)), risk may go well beyond classical toxicity, since they announce proliferation of intelligent nanoscale particles, that could reproduce by themselves.

Today, many people are afraid of the **violations of privacy** due to the extensive use of invisible modern technologies. They fear the nanotechnologies will violate their privacy with nanoscale sensors, which will render all our intimate and private life accessible to everybody. This could transform our world in a society of surveillance analogous to what was described in George Orwell's famous novel "1984" (Orwell 1949). This could also be worse if all the physiological mechanisms that take place in our body were continuously inspected and reported.

1.3 Specificity of Nanotechnology

One important question concerns the specificity of nanotechnology in general, and, more precisely, the specificity of the ethical issues straight to the development of nanotechnology. One currently argues that nanotechnology is nothing more than the prolongation of macromolecule chemistry. And, indeed, the difference between a nanoscale particle, for instance a nanosphere or a carbon nanotube, and a complex macromolecule is not easy to delineate.

Concerning nanotoxicity, nothing really distinguishes the study of the specific toxicity of nanoparticles from the study of the activity and toxicity of chemical products in general. As a consequence, nano-toxicity constitutes a subfield of classical toxicity studies. It goes the same with environmental consequences of nanotechnology, which look, to some respects, analogous to the consequences of chemical contaminations. The only real difference would be in the case of intelligent auto-replicating particles that adapt their behavior to the environment. But, even in such situation, nanoparticles would not fundamentally differ from biological agents like viruses or bacterias.

The situation for nanomedicine is not far from the one in medicine. Benefits of medical applications of nanotechnologies, for instance the use of nanosphere systems that can help to detect diseases or to transport chemotherapeutic drugs through the organism and to deliver into the brain (e.g. (Yu, Park, Jeong, Moon & Jon 2010)) – or into any well targeted location –, may thus be counterbalanced by the potential danger of nanoparticles for human health. This corresponds to the classical trade-off in the evaluation of drugs and ethical issues are the same.

1.4 Privacy

This paper deals with with privacy implications of nanotechnology. At first sight, the situation seems analogous to what happens with the other questions related to nanotechnology. For some people, the risks for privacy are of the same nature with nanotechnology than they were in the past with classical communication technologies that require to remain constantly vigilant, because of the risk of personal data theft and misuse, while others state that nanotechnology considerably amplifies the risks. There are even persons who assert that nanotechnology will make privacy protection obsolete, because of the proliferation of invisible sensors (Smith 2007).

For the use of nanotechnology in health care or handling environmental issues, adverse effects may be counterbalanced by beneficial effects and decisions

result from a cost-benefit evaluation. For the privacy issue the situation is quite different. There would be no obvious beneficial effects of nanotechnology enhancing privacy itself that could counterbalance privacy violation. In fact, as we shall see in the following, the beneficial effects that offset the risks for privacy don't concern the privacy itself, but the security of persons and the public transparency, which look to be highly desirable today. As a consequence, the privacy cannot be considered in isolation, without any other consideration; there is a necessary trade-off between privacy, security and transparency, that corresponds to what we call in the following the "ethical trilemma".

This paper contains a discussion about those various positions by making reference to the classical Panopticon that is an architecture for surveillance, which represents the total absence of privacy. The possible evolutions of the Panopticon due to the development of nanotechnology and, more generally, of convergent technologies are envisaged. In conclusion the new ethical conflicts generated by the development of nanotechnology, that constitute, as we argue here, an *ethical trilemma*, are discussed.

The paper is organized accordingly: after a first remind of the notion of privacy and a brief description of the classical Panopticon, in the second part the notion of *Nano-Panopticon* is presented. Then, a third part introduces the *digital Panopticon* and shows that, by potentiation with the Nano-Panopticon, it constitutes a *digital Nano-Panopticon*. Finally, the paper discusses the ethical issues that can be drawn from the consideration of those risks and the necessary trade-off between security, transparency and privacy that follows.

2 Privacy and Surveillance

2.1 Origin of the Notion of Privacy

In one of her most famous essay, *The Human Condition* (Arendt 1958), Hannah Arendt reminds the traditional distinction between the public and the private realm. She recalls that it comes from the Ancient Greece where the "public realm" was the place where state affairs were discussed and decided. From an urbanistic point of view, it corresponds to the *agora* in the Athenian city, i.e. to an open area where the freemen debated the questions of common interest. However, it was not restricted to a physical locus: the public realm was the symbolic place of political action, i.e. of freedom. By opposition, the private realm was devoted to labor and work, i.e. to the accomplishment of necessary things. The notion of "private realm" was then understood as synonymous of family in its extended significance, which included not only the atomic family, i.e. the father, the mother and the children, but the grand-parents, the cousins, the aunts and uncles, and also the servants who were for many of them slaves. The private realm was entirely dedicated to the subsistence. It was there that people were organizing to cultivate, hunt, raise animals, build and repair houses etc. This realm was totally submitted to the achievement of material constraints of life.

In its contemporary meaning, the notion of privacy comes from the end of the 19^{th} century. Its original aim was to restrict the public dissemination of details relating to a person's private life in the context of the development of press and publicity allowed by the invention of photography and newspapers. It then

appeared necessary to recognize the right to be alone and the moral integrity of the person. Afterwards, the protection of the "right to one's personality" has been explicitly stipulated (Warren & Brandeis 1890) under the name of privacy.

Note that the feeling of the individual didn't suddenly appear at the end of the 19^{th} century. Before, there were many people wanting to express their individuality through their life or their creation. It was the case in the Antiquity and, especially, in the Modern Age, with the rise of the individualism. However, for centuries, because of the material constraints, especially because of the exiguity of living spaces, only a few educated and rich persons had the ability to care of their self and of their privacy. It's only, by the end of the 19^{th} century, that this requirement became collective in western developed societies (Langelier 2004).

The development of modern communication technologies and of sensors, e.g. microphones, video cameras and web-cams, during the 20^{th} century encouraged invasion of privacy and violation of *personality rights*[2]. Obviously, there is no strict causality relation between the development of modern communication technologies and the threat for privacy and personality rights, but these techniques afford many opportunities to threaten privacy to states, to criminals or even to idealists like, for instance, Julian Assange, the founder and editor in chief of WikiLeaks.

This leads philosophers to describe in more details some main interests in the protection of privacy rights, for instance, the intrusion into a person private affairs, the public disclosure of embarrassing private facts about an individual or the publicity placing one in a false light in the public eye. Briefly speaking, the privacy protection is based on a general principle according to which everyone has the right to totally control his personal information, i.e. to decide what information he/she accepts to reveal, when and to whom he/she does it. However, this general principle is difficult to apply. For instance, in France, in the case of the image – e.g. in the case of photos or videos – of a person in public, the French notion of "droit à l'image" allows persons to dispose of their image. This "droit à l'image", which does not exist in UK legislation, conflicts with the freedom of expression and the freedom of press, which permit journalists to take pictures in the public space. As a consequence, depending on the context, it can be either prohibited or allowed to take pictures of persons in public without their permission.

In addition, note that, in this narrow view, the protection of privacy is restricted to the individual control over personal information dissemination. However, privacy is a more general and essential notion that is related to the idea of intimacy, i.e. to the close, familiar, and affectionate personal relationship with another person or within a group. Privacy is necessary for intimacy, without intrusion or observation, which plays a key role in the development of the moral and social personality of individuals able to respect, love and trust. As such, it also needs to be protected.

[2]The notion of *personality rights* is a technical legal term that can simply be defined as the right of an individual to control the commercial use of his/her name, image, likeness or other unequivocal aspects of one's identity.

2.2 The Panopticon

The Panopticon was designed at the end of the eighteenth century by Jeremy Bentham as a piece of prison architecture (Bentham 1838) that was supposed both to decrease the cost of surveillance and to improve its efficiency. It characterizes a rationally organized prison society where the detainees cannot vindicate any right to protect their individual intimacy because they have been judged so bad that they need to be continuously surveyed and educated. Briefly, the Panopticon is built on a ring around a central tower, where prison guards can see everything their prisoners do without being viewed by them. The cells are transparent, they receive and transmit sunlight. In that way, inspectors may observe the prisoners' every movement without being seen. Because the prisoners don't see their guards, the fear to be observed is sufficient to overawe them, even when nobody is watching. Moreover, the prisoners are totally isolated from each other and, consequently, they don't communicate.

The Panopticon played a central role in modern societies. It was not restricted to the surveillance of prisoners. Key institutions of the modern age like factories, hospitals, asylums and even schools were organized on this model. The original paper of Bentham explicitly refers to all those institutions[3]. Later on, many philosophers, among them Michel Foucault in *Discipline and Punish* (Foucault 1977), described it as a typical device ("dispositif" in French) of the modern legal state, i.e. a social arrangement that summarizes the underlying political structure of the society, as it threatens all the deviants, i.e. criminals that are put in jail, sick persons in hospitals, mad locked up in asylums, etc.

The Panopticon defines a structural schema that is diametrically opposed to the idea of protection of privacy. This is the reason why it has been referred by those who fear the possible violations of privacy. But, it has not been uniquely designed to imprison, i.e. to efficiently protect the society against the violation of the rights; it can also serve to cure people. It has even been seen as a model of organization on which many institutions of the modern society were shaped in the state of right as it appears in the 18^{th} and 19^{th} century revolutions. Lastly, the original Panopticon model was not supposed to be generalized to the overall society except later, with some deviations like the one developed in the Orwell's novel entitled "1984" (Orwell 1949).

Despite the positive role that might play the Panopticon for public health and respect of law, it clearly conflicts with the privacy protection that has emerged at the end of the 19^{th} century. On one side, the Panopticon is a way to protect individuals, on the other side, it considerably restricts their freedom and their right to privacy, which is an essential condition of the freedom. This is the reason why it is so interesting for our purpose: indeed, it is emblematic of the lack of privacy in the former modern societies, more precisely in the modern societies that appear between the end of 18^{th} century and the 20^{th} century, and, as such, it will help us, in the following, to understand the new nature of privacy violations that follows the development of nanotechnology and, more generally, of converging technologies.

[3]To be more precise, the title of the Bentham's essay on the Panopticon (cf. (Bentham 1838)) lists some of the institutions of which the organization could be built on the Panopticon model that are *Penitentiary-Houses, Prisons, Houses of Industry, Work-Houses, Poor-Houses, Manufactories, Mad-Houses, Lazarettos, Hospitals and Schools*

3 Nano-Panopticism

3.1 Invisible Surveillance

The major privacy related issue of nanotechnology is its potential to considerably extend surveillance with nanoscale devices, which become invisible and unperceivable by the individuals. In a paper untitled "On Nano-Panopticism: A Sociological Perspective" (Mehta 2003), Michael Mehta investigates the social consequences of the proliferation of micro sensors. With such devices disseminated everywhere in houses, in streets, in clothes, etc., the utopia of a total visibility would become a reality. It would then be possible to achieve a perfect Panopticon where prisoners would be continuously under the gaze of guards.

This prospect is certainly very distant from what the current state of the art allows. In particular, it presupposes that all the recorded data could be analyzed, which, even with the help of powerful data mining techniques, remains today totally intractable. However, seen as a prospective view of the future of nanotechnologies, it shows how the developments of converging technologies might entail a total lack of privacy if nobody is taking care.

3.2 Internal Panopticon

In addition to this "external Nano-Panopticon", which allows to record all the movements of individuals, researchers imagine to build an "internal Nano-Panopticon" by implanting nano-devices controlled by microchips in human body (Aubert 2011). Some of these devices could deliver drugs or aid Alzheimer's patients with assisted cognition devices. Some others would continuously record physiological parameters. For instance, it is mentioned gold nanoparticle probes that might allow earlier cancer detection (Wang & Ma 2009, Yu et al. 2010, Cheng, Cuda, Bunimovich, Gaspari, Heath, Hill, Mirkin, Nijdam, Terracciano, Thundat & Ferrari 2006). More generally, implantable medical diagnostic tools could help to establish a self-monitoring of physiological well-being and dysfunctions. In the NSF report on converging technologies edited by M.C. Roco and W.S. Bainbridge (Roco & Bainbridge 2003), the development of implantable sensors or "smart" patches that regulate drug delivery or heart rate is mentioned. It is said that "Such sensors might monitor, for example, blood chemistry, local electric signals, or pressures." and that "The sensors would communicate with devices outside the body to report results, such as early signals that a tumor, heart damage, or infection is developing."

Mentioned by (Roco & Bainbridge 2003), the implantation of chips in a person's brain could send neural signals from brain areas to control exoskeleton or prosthetic robotic arms. According to this report, it could help to restore or to augment fundamental motor functions such as grabbing, reaching and walking. It could also help to record and to archive individual neural activities. In this respect, existing Brain-Computer Interfaces could certainly be greatly improved by the nano-sensors directly implanted in the brain.

Note that the NSF report edited by Roco and Bainbridge (Roco & Bainbridge 2003) was a visionary statement of which role was to motivate new researches. The present reality doesn't correspond to this vision. Nevertheless, we mention this report here, since the role of this paper is to envisage the question of privacy in the future, and not only in the present time, where the development of

nanotechnology doesn't yet alter our privacy. More generally, some of the most frightening scripts of invasion of privacy have to be envisaged, even if there is no actual risk with the today development of technology.

3.3 Metamorphosis of the Panopticon

In brief, nanotechnology contributes to the surveillance at three levels.

First, it prolongs the classical surveillance techniques by developing Radio Frequency Identity Chips (RFIDs) (Aubert 2011), invisible tags and nano-sensors that are able to record and to trace individuals movements (Avoine & Oechslin 2003). With the proliferation of unapparent video-cameras build with nano-sensors (Liua, Zhang, Wana, Jianga, Taoa, Lia, Gonga & Tanga 2008) and their dissemination, it considerably extends the classical Bentham's Panopticon, without fundamentally changing its nature.

Second, with inner surveillance techniques that make intrusion in the body, the oversight goes beyond the classical observation of one's move. It's not only a question of intensity of sensors; it's the nature of surveillance that is changing: it's becoming possible to continuously observe biological modifications that affect our body and that are invisible to our own consciousness. As a consequence, the surveillance techniques help us to know us better than we would do it by ourselves. In this respect, this second level overtakes the classical logic of surveillance of which the Bentham's Panopticon was emblematic. On the one hand, it certainly corresponds to a very interesting evolution of surveillance, which might be very beneficial in the future, because it could lead to improve health care and security in the population. On the other hand, the risk might be that this knowledge of ourselves by others – e.g. by physicians and/or by the administration – escapes to our control.

Furthermore, a third level might allow to directly capture the brain signal, to automatically interpret it and then to get direct access to the thoughts. If this were actually true, this would certainly lead to intrude into our deepest intimacy to an unthought degree. Nevertheless, despite of the recent progresses in functional Brain imagery and in the Brain-Machine Interfaces, it seems that presently we are yet far away from being able to realize such devices with the current development of technology. One of the main impediments is the difficulty to analyze and to understand the meaning of the considerable mass of data generated by brain signals. Maybe, in the future, it could happen that the progresses of data mining would make those data comprehensible and thus, our most intimate thoughts transparent to anyone. Note that this visionary view is not new. For instance, Vannevar Bush in the conclusion his famous paper "As we may think" (Bush 1945) had developed a similar idea: he has imagined that one day the MEMEX – i.e. the external memory made of electronic devices – might be directly plugged to our brain. Obviously, if it would be accessible, this third level of surveillance would exceed again the second level to the point that no privacy at all – and consequently no intimacy – would remain possible. But, we are so distant from such an achievement that there is no need to deepen further on this point.

To conclude, nanotechnology enhances heavily the degree of surveillance of the classical Panopticons, which are metamorphosed in what we call, following Michael Mehta (Mehta 2003), *Nano-Panopticons*. These Nano-Panopticons not only increases the amount of surveillance; they also transform the nature of

surveillance; they make evolve the old centralized logic of surveillance, of which the architecture of Panopticon was emblematic, into a new decentralized logic of surveillance (van den Hoven & Vermaas 2007) that is decribed in the next chapter.

4 Extensions within Digital Panopticons

4.1 Extension to Digital World

Both the beneficial effects of the information gathered by implanted nano-sensors and the possible privacy harms due to a misuse of this information directly depend on interpretation processes. Due to the enormous mass of information, this interpretation cannot be done manually. Computers are required to help to understand the meaning of a so huge quantity of information. Furthermore, it is necessary to commission people to intervene when required, for instance to cure patients who are diagnosed or to prohibit deviant behaviors. Without this social environment of services, nanotechnology is useless. This means that nanotechnology cannot be understood isolated. It has to be associated with communication technologies, with computers, with data mining processes and with human organizations. In other words, nano-devices — and more especially nano-sensors — are part of *computing artefacts*, because they include automatic computers to deal with the generated data. They are also *socio-technical systems*, because their usefulness directly depends on the social organizations that allow to build the necessary infrastructures that are required to exchange data and to act appropriately. As a consequence, the nano-Panopticons that were described in the previous section need to be extended to the digital world, i.e. to the human world surrounded by computers and networks.

4.2 Digital Panopticons

Besides the use of nanotechnology, web-cams, RFID tags and many other recent information technology devices render now possible to record and to broadcast an increasing part of anybody's daily activities (Bailey & Kerr 2007, Mitton & Simplot-Ryl 2011). As soon as a mobile phone is switched on, it is easy to identify and localize its owner. The Location-Based Services (Joore 2008), which have been perceived as an incredible contribution to individual empowerment, allow for continuously tracking any of our movements. In many developed countries, personal data concerning health, employment, income, travel and digital communications are officially recorded and stored in databases (Lahlou 2008). It is then in principle possible to fuse (Laudy, Ganascia & Sedogbo 2007) all those data using modern data mining techniques. Therefore, most of our personal data that are now becoming available within digital media could be merged. As such, they might be easily divulged throughout the world and exploited.

Certainly, there are national legislations that protect privacy and that preclude such a merge and *a fortiori* such a divulgation, for instance in France the law "Informatique et liberté". Simultaneously, there are attempts to open access to data, without infringing privacy. As an illustration, the "open data" movement tends both to anonymize data and to make them more publicly avail-

able. Therefore, the digital world becomes more and more transparent because huge amounts of data may be accessible anywhere all over the world through Internet and there exists a social aspiration to public access to data.

In a way, this digital world seems to be analogous to the Bentham's Panopticon, because all the personal data seem to be accessible, which makes it transparent, even if individuals have acquired the right to protect some of their data. But, there is no more limit to its extension, which is no longer restricted to a building, like a prison or an hospital, nor localized to specific place. As a consequence, digital technology gives birth to what has been called the *digital Panopticon*, which extends, to the entire planet, the scope of the classical Panopticon. In addition, the digital Panopticon makes the data available to many people and not just to a few guards, as in the original Bentham's Panopticon.

4.3 Potentiation

In medicine, the notion of *potentiation* designates the enhancement of a drug effect due to biochemical interactions with other drugs or environmental conditions. By analogy, nanotechnology and digital technology mutually potentiate each other, which could give birth to an hybrid of the Nano-Panopticon and the digital Panopticon that we call the *digital Nano-Panopticon*.

On the one hand, nanotechnology has the potential to tremendously enhance computer technology by increasing computing power and storage capacity of electronic devices. Available technologies allow to reach in industry size of order of 22 nanometers while in laboratory much smaller components can be fabricated.

Recently, in February 2010, Professor Jean-Pierre Colinge, from the Tyndall National Institute in Cork, Ireland announced a breakthrough in transistors with the design and fabrication of the world's first junctionless transistor that can be produced at 10-nanometer (Colinge, Lee, Afzalian, Akhavan, Yan, Ferain, Razavi, O'Neill, Blake, White, Kelleher, McCarthy & Murphy 2010).

On the other hand, coupling the nanotechnology to digital world would make them considerably more powerful. The coupling of nano-devices with "nano-chips" would increase their efficiency. For instance, drug delivery nano-spheres could adapt their behavior to physiological parameter, by an automatic computation. Moreover, the interpretation of the data recorded by nano-sensors requires an intense computing power that the enhancement of computer technology due to the use of nano-devices may certainly contribute to afford.

This mutual potentiation of nanotechnology and digital technology amplifies the threats for privacy protection. We may fear the erection of *Neo-Panopticons* — or *digital Nano-Panopticons* — that are hybrids of Nano-Panopticons, Digital Panopticons and Bio-Panopticons, i.e. Panopticons built with biotechnologies for the permanent and continuous surveillance of living organisms justified both by health care and environmental protection concerns.

Undoubtedly, in such a context, it would be more and more difficult to ensure the privacy protection. Without going in a catastrophic scenario by showing the danger of digital Nano-Panopticons, the classical notion of privacy protection, according to which anyone is the owner of all the data about his/her private life is evolving. This justifies the arguments of those, like Robert Ellis Smith, the publisher of the *Privacy Journal* newsletter, who argue (Smith 2007) that

the new environment of nanotechnology may render obsolete the old regime of protecting privacy. More generally, considering that the notion of privacy protection is quite recent in the history of humankind, it would be possible to live in a world with new privacy regulation rules, which would substantially differ from the classical ones that are inherited from the end of the 19^{th} century.

5 Towards the End of Privacy?

Let us summarize our argument. First of all, we have recalled that the notion of privacy protection is historical and that its apparition during the 19^{th} century is more or less concomitant with the systematization of the surveillance (cf. section 2.1). It is as if there were a dialectical link between privacy and surveillance, which makes the need for privacy protection increase when the surveillance is widespread. We have then shown that, with the development of nano-technology and with its coupling with information technology and biotechnology, i.e. with the development of converging technologies, the nature of surveillance is evolving (cf. section 4). On the one hand, it becomes technically possible to follow and to trace everyone movements. On the other hand, the amount of generated data and the easiness with which everyone can now catch and spread information, change the nature of surveillance, which according to van den Hoven et al. (van den Hoven & Vermaas 2007) becomes decentralized. Our underlying hypothesis is that this evolution of the surveillance, i.e. the change-over from a centralized to a decentralized surveillance, greatly affects the need for privacy protection. We envisage in this section the new status of privacy protection that derives from those evolutions.

5.1 The Ethical Limit of Privacy

Is privacy always suitable? The question may cause surprise, because the right to privacy seems to be largely recognized as fundamental, but there exist people (Posner 1981, Parent 1983, Thomson 1975) scrutinizing the notion of privacy and blaming, for ethical reason, the emphasis put on it. Some of the detractors are philosophers (Posner 1981, Parent 1983) who argue that the known privacy violation cases can be analyzed in terms of violation of property rights or violation of the person rights. As a consequence, the concept of privacy is a mixture, which is not really distinctive and which does not really help to rule behavior. Other, for instance feminists (MacKinnon 1989), say that privacy has a dark side, because it can be used as a shield to eclipse cases of domination, degradation, harassment and abuse of persons, especially of women and children.

These objections do not totally reject any idea of privacy protection, but they aim at targeting its theoretical justifications in order to see if it is not an instance of a more general right of the person, like the right to security. It is of particular importance in a time where the state of technology makes privacy necessarily evolve. In other words, the focus is to understand the ethical limits of privacy, while the development of technology raises doubts on the classical view of informational privacy considered as the ability to fully control on its own personal data.

5.2 Surveillance vs. Sousveillance

More generally, one currently argues that the full disclosure of all public and private information contributes to establish a state of total transparency in society that is desirable. According to these ones, for instance to Steve Mann, this would not really strengthen the logic of surveillance and lead to a generalized surveillance society, but would instead contribute to institute a new regime, described as a "sousveillance" (Mann, Nolan & Wellman 2003, Ganascia 2009), in which powerful people are permanently observed by those they are supposed to dominate. The word "sousveillance" is a neologism built on the model of "surveillance", the latter from French "sur", meaning "over" and "veiller", "to watch", and which literally means "watching from above". By analogy, sousveillance has been built to designate the act of watching ("veiller") from below ("sous"). In the case of sousveillance, the watchers are socially below those who are watched, while in the case of surveillance it is the opposite, they are above.

Note that the original notion of sousveillance promoted by Steve Mann signifies that every watcher would voluntarily give free access to all information recorded. Usually, people recording information take part in the event and participants are aware of the recording. According to Steve Mann and to others, this would lead to a more balanced world state of justice, since everybody would act as if he was observed by others (Munro 2000). Moreover, the sousveillance would help to denounce abuse or to check the conformity of public goods. For instance, Steve Mann shows how, with a camera in his pocket, he can record violation of the electrical code (cf. `http://wearcam.org/password-66-450.htm`) and make it publicly known. However, in that case, it may happen that people disagree with the information capture and attempt to destroy the camera. On the other hand, if someone has been wrongly accused, it would always be possible to show his records to be free from doubts. As an illustration, let us recall the story of Rodney Bradford. This 19 years old man has been arrested and held for 12 days for an armed robbery on October 17^{th} 2009 of two people in the Brooklyn housing project where he lives. He has then been exonerated thanks to a status update he posted on social networking site Facebook. The message on Rodney Bradford's Facebook page, posted at 11:49 a.m. on October 17^{th}, asked where his pancakes were. The words were typed from a computer in his father's apartment in Harlem.

5.3 Transparency vs. Privacy

Those examples and the subsequent discussions show that many of our contemporaries share the aspiration to a total transparency, which seems to mismatch the need for privacy protection. Let us remind another recent illustration of such a conflict between transparency and privacy. It took place by the end of 2010 when 400,000 of secret telegrams containing embarrassing information about American, European and Middle-East foreign policies were divulged to newspapers by the WikiLeaks organization. Among these, there were private declarations of statesmen and confidential assessments of diplomats expressing their personal feelings about the governments of the countries they had visited. The diplomacy of the United-States of America and of some other countries has been called into question by what people were calling the *Cablegate*, by analogy to the *Watergate*. Modern democracies, and especially the United-States of

America, were hampered; as sovereign states, they were facing a novel dilemma. On the one hand, last few years, many of them have tried to open the public data to all citizens. This tendency is present in Europe and in the United-States of America. For example, once elected, Barak Obama has promoted the *Open Government*(Obama 2009), which makes all the administrative data — i.e. heath inquiries, environmental records, public funding etc. — available to everybody. On the other hand, states are used to deal with many matters, especially in the diplomatic area, either in secrecy, or, at least, in a discrete way. As a consequence, they can't easily accept the public disclosure of top secret information.

5.4 The New Ethical Trilemma

For summarizing, let us recollect the different steps of our analysis. After recalling the scope of the notion of privacy (cf. section 2.1), we have examined the impact of the development of contemporary nanotechnology on privacy protection (cf. section 3). We saw that this study cannot be envisaged without taking into account the mutual potentiation of nanotechnology, information technology and biotechnology (cf. section 4.3). It then appeared that the surveillance has been evolving not only in intensity, but also, in its organization, which becomes more and more decentralized (cf. 5.1). The notion of sousveillance and its generalization to the overall society help to understand the present evolution. More precisely, the logic of surveillance, which corresponds to a vertical cast of information, coexists more and more often with a logic of sousveillance that leads to an horizontal spread of information.

Lastly, we also noticed that privacy protection was directly related to the surveillance organization. As a consequence, we can hypothesize that the principles on which privacy protection is based are changing, because now the privacy is not only related with a centralized surveillance organization, but also with a decentralized sousveillance schema. The definition of privacy itself should considerably evolve in the future due to the above mentioned development of converging technologies. In particular, the idea according to which everybody should control his/her personal data becomes more and more untenable.

In addition to these technical impediments to a full privacy protection, criticisms have been addressed to the focus on privacy protection (cf. 5.1). Some argue that privacy is an instance of more fundamental rights of the person while others mention some requirements that may interfere with privacy. For instance, health care and security could necessitate full traceability of both motions and physiological parameters of individuals, which becomes possible with digital convergence, i.e. with the coupling of nanotechnology, digital technology and biotechnology. The socio-technical systems that are erected to ensure the continuous recording and the exploitation of traces of individual behaviors, inevitably conflict with privacy protection requirements. However, security and privacy equally answer to a demand of most of our contemporaries. Therefore, between the privacy protection need and the security exigency, there is a tension.

Moreover, as we already mentioned, besides this first tension, there exists a second tension between privacy protection and the aspiration to transparency. And, not only, privacy protection and security of persons on the one hand, and privacy protection and transparency on the second hand, are conflicting, but also

security and transparency, which has appeared obvious during the WikiLeaks affair, when the information divulged by the WikiLeaks website had deleterious consequences both for the security of persons and for state policy. Therefore, we could also add a third tension, between security of persons and the need for transparency. Note that the first tension, i.e. the tension between privacy protection and security, existed since the origin of the privacy protection, in the end of the 19^{th} century, while the second and the third tension, between privacy protection and transparency on the one hand and between security and transparency on the other hand are quite recent, because they are due to the need for transparency and to the ease with which everybody can divulge information now. As a result of those three tensions, there is now a necessary trade-off between privacy, security and transparency.

To illustrate this point, let us take an example of this necessary trade-off between privacy, security and transparency. Suppose that, as we suggested earlier (cf. section 3.2), the development of converging technologies would render possible a preventive detection of diseases by the use of medical sensors that might monitor blood chemistry, local electric signals or pressures and communicate with communication devices to report results, such that a tumor, a heart damage, or infection is developing. Such recorded data need physicians to be interpreted, but the privacy protection requirements mean that confidentiality be ensured.

To conclude, we are now facing a *new ethical trilemma* that is a choice between three mutually exclusive ethical options: security, transparency and privacy. None of the three options can be totally privileged. Therefore, it's necessary to continuously arbitrate between them, because the development of modern technologies, especially of nanotechnology and digital technology, makes them both conflicting and equally suitable.

References

Arendt, H. (1958), *The Human Condition*, University of Chicago Press, Chicago, USA.

Aubert, H. (2011), 'Rfid technology for human implant devices', *"Comptes rendus à l'Académie des Sciences", Special issue on nanosciences/nanotechnologies*.

Avoine, G. & Oechslin, P. (2003), Rfid traceability: A multilayer problem, Technical report, EPFL, Lausanne, Switzerland. [On-line]. Available at `http://fc05.ifca.ai/p11.pdf`, accessed June 2011.

Bailey, J. & Kerr, I. (2007), 'The experience capture experiments of ringley & mann', *Ethics and Information Technology* **9**(2), 129–139.

Bentham, J. (1838), *The Work of Jeremy Bentham*, Vol. 4, William Tait, London, chapter "Panopticon ; or, The Inspection House : Containing the Idea of a New Principle of Construction Applicable to Any Sort of Establishment, in Which Persons of Any Descriptions are to be Kept under Inspection and in Particular to Penitentiary- Houses, Prisons, Houses of Industry, Work-Houses, Poor- Houses, Manufactories, Mad-Houses, Lazarettos, Hospitals and Schools", pp. 37–172.

Bush, V. (1945), 'As we may think', *Atlantic Monthly* **176**(1), 641–649.

Cheng, M. M., Cuda, G., Bunimovich, Y. L., Gaspari, M., Heath, J. R., Hill, H. D., Mirkin, C. A., Nijdam, A. J., Terracciano, R., Thundat, T. & Ferrari, M. (2006), 'Nanotechnologies for biomolecular detection and medical diagnostics', *Curr Opin Chem Biol* **10**(1), 11–9. 1367-5931 (Print) Journal Article Research Support, N.I.H., Extramural Research Support, U.S. Gov't, Non-P.H.S. Review.

Colinge, J.-P., Lee, C.-W., Afzalian, A., Akhavan, N. D., Yan, R., Ferain, I., Razavi, P., O'Neill, B., Blake, A., White, M., Kelleher, A.-M., McCarthy, B. & Murphy, R. (2010), 'Nanowire transistors without junctions', *Nature Nanotechnology* **5**, 225–229.

Foucault, M. (1977), *Discipline and Punish*, Vintage, New-York.

Ganascia, J.-G. (2009), *Voir et pouvoir: qui nous surveille?*, Editions du Pommier, Paris.

Hillie, T. & Hlophe, M. (2007), 'Nanotechnology and the challenge of clean water', *Nat Nano* **2**(11), 663–664.

Joore, P. (2008), 'Social aspects of location-monitoring systems: the case of guide me and of my-sos', *Social Science Information* **47**(3), 253–274.

Joy, B. (2000), 'Why the future doesn't need us', *Wired Magazine*. cf. www.wired.com/wired/archive/8.04/joy.html.

Lahlou, S. (2008), 'Cognitive technologies, social science and the three-layered leopardskin of change', *Social science information* **47**(3), 227–251. `http://ssi.sagepub.com/cgi/content/abstract/47/3/227`.

Langelier, R. E. (2004), 'Prolgomnes une recherche sur la vie prive dans une perspective historique et sociologique', *Lex Electronica*. `http://www.lex-electronica.org/articles/v9-2/langelier.htm`.

Laudy, C., Ganascia, J.-G. & Sedogbo, C. (2007), High-level fusion based on conceptual graphs, *in* 'Proceedings of the 10^{th} international Conference on information fusion', Quebec, Canada.

Liua, W., Zhang, J., Wana, L., Jianga, K., Taoa, B., Lia, H., Gonga, W. & Tanga, X. (2008), 'Dielectrophoretic manipulation of nano-materials and its application to micro/nano-sensors', *Sensors and Actuators B: Chemical* **133**(2), 664–670.

MacKinnon, C. (1989), *Toward a Feminist Theory of the State*, Harvard University Press, Cambridge.

Mann, S., Nolan, J. & Wellman, B. (2003), 'Sousveillance: Inventing and using wearable computing devices for data collection in surveillance environments', *Surveillance & Society* **1**(3), 331–355.

Marano, F., Lahmani, M. & Houdy, P., eds (2011), *Nanoethics and Nanotoxicology*, Vol. Tome 4, Springer.

Mehta, M. (2003), On nano-panopticism: A sociological perspective, Technical report, University of Saskatchewan, Online. available at http://chem4823.usask.ca/~cassidyr/OnNano-Panopticism-ASociologicalPerspective.htm.

Mitton, N. & Simplot-Ryl, D. (2011), 'From the internet of things to the internet of physical world', *"Comptes rendus à l'Académie des Sciences", Special issue on nanosciences/nanotechnologies*.

Munro, I. (2000), 'Non-disciplinary power and the network society', *Organization* **7**(6), 79–95.

Obama, B. (2009), Transparency and open government, Memorandum for the heads of executive departments and agencies, The White House, Washington, USA. http://www.whitehouse.gov/the_press_office/Transparency_and_Open_Government/.

Orwell, G. (1949), *Nineteen Eighty-Four. A novel.*, Harcourt, Brace & Co., New-York.

Parent, W. (1983), 'Privacy, morality and the law', *Philosophy and Public Affairs* **12**(2), 69–88.

Posner, R. (1981), *The Economics of Justice*, Harvard University Press, Cambridge.

Roco, M. & Bainbridge, W., eds (2003), *Converging technologies for improving human performance: Nanotechnology, biotechnology, information technology and cognitive science*, Kluwer Academic Publishers (Springer), Doredrecht, Boston.

Smith, R. E. (2007), 'Scary stuff', *Forbes*. http://www.forbes.com/2007/11/21/privacy-surveillance-technology-oped-cx_res_1126privacy.html.

Stern, S. T. & McNeil, S. E. (2008), 'Nanotechnology safety concerns revisited', *Toxicological Sciences* **101**(1), 4–21.

Thomson, J. (1975), 'The right to privacy', *Philosophy and Public Affairs* **4**, 295–314.

van den Hoven, J. & Vermaas, P. E. (2007), 'Nano-technology and privacy: On continuous surveillance outside the panopticon', *Journal of Medicine and Philosophy* **32**(3), 283–297.

Wang, Z. & Ma, L. (2009), 'Gold nanoparticle probes', *Coordination Chemistry Reviews* **253**(11-12), 1607 – 1618. http://www.sciencedirect.com/science/article/B6TFW-4VCNP9H-2/2/b66681e54f88b82d8c1f89fd90e33d5f.

Warren, S. & Brandeis, L. (1890), 'The right to privacy', *Harvard Law Review* **4**, 193–220.

Yu, M. K., Park, J., Jeong, Y. Y., Moon, W. K. & Jon, S. (2010), 'Integrin-targeting thermally cross-linked superparamagnetic iron oxide nanoparticles for combined cancer imaging and drug delivery', *Nanotechnology*.